ABSTRACT OF THE DISCLOSURE

Secure key exchange and protected content distribution between a first entity and a second entity in a processing system may be accomplished by generating, by the first entity, a first key, encrypting the first key with a public key of a third entity, and storing the encrypted first key in the third entity. The second entity generates a second key, encrypts the second key with the public key of the third entity, and stores the encrypted second key in the third entity. The third entity decrypts the encrypted first key and the encrypted second key, using the third entity's private key to obtain the first key and the second key, encrypts the first key using the second key, and stores the first key encrypted by the second key in the third entity. The second entity then obtains the first key encrypted by the second key, and decrypts, using the second key, the first key encrypted by the second key. The first key may then be used to encrypt content sent to from the second entity to the first entity.